

Cisco Jabber e modalità SIP OAuth

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Restrizione](#)

[Premesse](#)

[Vantaggi principali](#)

[Architettura generale](#)

[Configurazione - Jabber locale](#)

[1. Configurare i login di aggiornamento.](#)

[2. Configurare le porte OAuth.](#)

[3. Abilitare la modalità OAuth SIP.](#)

[4. Riavviare il servizio Cisco CallManager.](#)

[5. Configurare il supporto OAuth nel profilo di sicurezza.](#)

[Configurazione - Jabber over MRA](#)

[Prerequisiti](#)

[Passaggio 1. Abilitare Aggiorna login su MRA.](#)

[Passaggio 2. Aggiornare i nodi CM unificati in Expressway-C.](#)

[Passaggio 3. Configurare il supporto OAuth nel profilo di sicurezza.](#)

[Verifica](#)

[1. Verificare se la modalità OAuth SIP è abilitata a livello globale.](#)

[2. Verificare che le voci SAN Expressway-C siano state inserite correttamente in CUCM.](#)

[3. Verificare le zone CEOAuth in Expressway-C.](#)

[4. Verificare che il processo CallManager sia in ascolto sulle porte SIP OAuth.](#)

[Risoluzione dei problemi](#)

[Esempio di registro Jabber \(locale\)](#)

[Scenario 1 - Mancata corrispondenza della porta di registrazione SIP OAuth](#)

[Scenario 2 - CA sconosciuta da Expressway](#)

[Scenario 3 - CA sconosciuta da UCM](#)

Introduzione

In questo documento vengono descritte la configurazione e le procedure di base per la risoluzione dei problemi e l'implementazione della modalità SIP OAuth con Cisco Jabber.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Registrazione softphone Jabber
- Unified Communications Manager (UCM)
- Soluzione MRA (Mobile and Remote Access)

Componenti usati

Versione minima del software per il supporto della modalità SIP OAuth:

- Cisco UCM 12.5
- Cisco Jabber 12.5
- Cisco Expressway X12.5

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Restrizione

Quando la modalità SIP OAuth è abilitata, le opzioni Abilita autenticazione digest e Configurazione crittografata TFTP non sono supportate.

Premesse

Vantaggi principali

La protezione della segnalazione SIP e dei supporti per il softphone Cisco Jabber richiede attualmente più passaggi di configurazione. Il più difficile consiste nell'installare e rinnovare i certificati client (LSC), soprattutto se un dispositivo Cisco Jabber sta passando da un sistema locale a un altro, e mantenere aggiornati i certificati all'interno del file CTL.

La modalità SIP OAuth consente a Cisco Jabber Softphone di utilizzare token autodescrittivi OAuth anziché il certificato LSC client per l'autenticazione su un'interfaccia SIP protetta. Il supporto di OAuth sull'interfaccia SIP UCM consente la segnalazione e i supporti sicuri per le installazioni Jabber on-premises e MRA senza la necessità di modalità mista o CAPF.

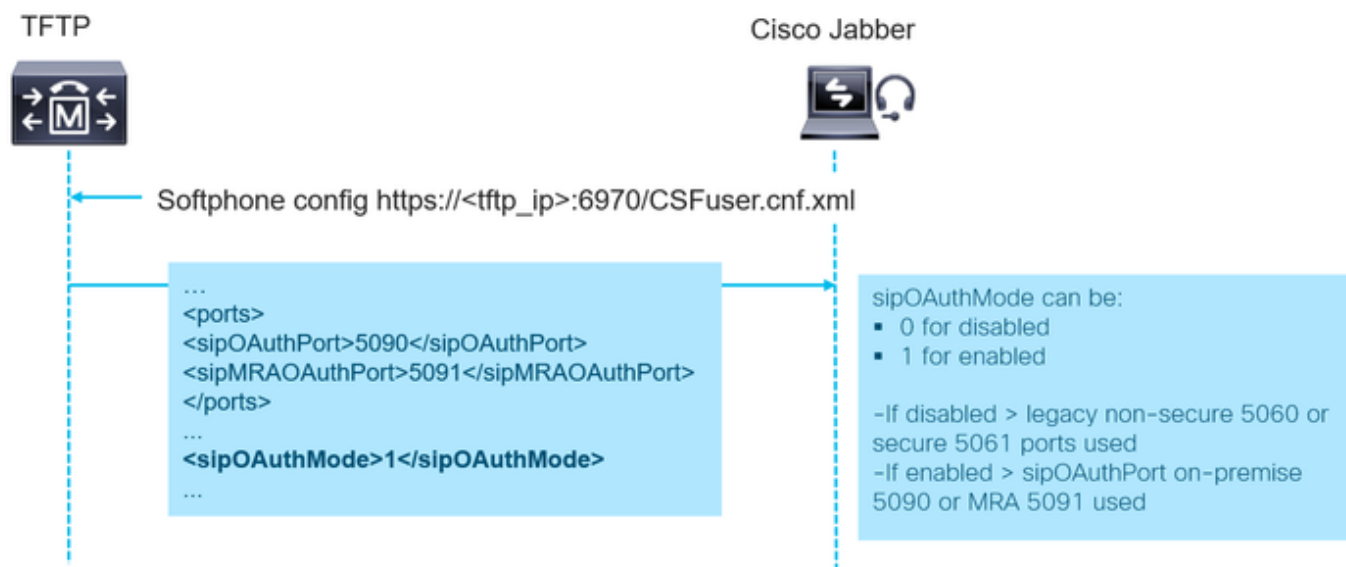
Principali vantaggi del supporto della modalità SIP OAuth per Cisco Jabber:

- Abilita la crittografia sempre attiva senza sovraccaricare l'amministratore.
- Segnalazione e supporti sicuri per Cisco Jabber senza la necessità della modalità mista (nessun aggiornamento CTL, manutenzione dei certificati, ecc.)
- Non è necessario installare e mantenere LSC sui client Jabber.
 - Problemi con LSC su più dispositivi (notebook/dispositivi mobili...)

- L'operazione CAPF è necessaria ogni volta che Jabber viene installato su un nuovo dispositivo.
- Operazione CAPF non supportata su MRA.

Architettura generale

Il dispositivo Cisco Jabber riconosce che l'autenticazione OAuth è abilitata sull'interfaccia SIP analizzando il file di configurazione CSF (<http://<cucmIP>:6970/<CSF-device-name>.cnf.xml>), esempio di file di configurazione (alcune righe non sono disponibili per brevità):



Cisco Jabber legge il parametro `sipOAuthMode` per determinare se la modalità OAuth SIP è abilitata o meno. Questo parametro può assumere uno dei seguenti valori:

- 0 - OAuth SIP disabilitato
- 1 - OAuth SIP abilitato

Se la modalità SIP OAuth è abilitata, Jabber utilizza uno di questi parametri per determinare la porta per la connessione SIP TLS - `sipOAuthPort` per le distribuzioni locali o `sipMRAOAuthPort` per le distribuzioni basate su MRA. Nell'esempio vengono presentati i valori predefiniti - `sipOAuthPort 5090` e `sipOAuthPort 5091`. Questi valori sono configurabili e possono essere diversi su ciascun nodo CUCM.

Se la modalità SIP OAuth è disabilitata, Jabber utilizza le porte legacy non sicure (5060) o sicure (5061) per la registrazione SIP.

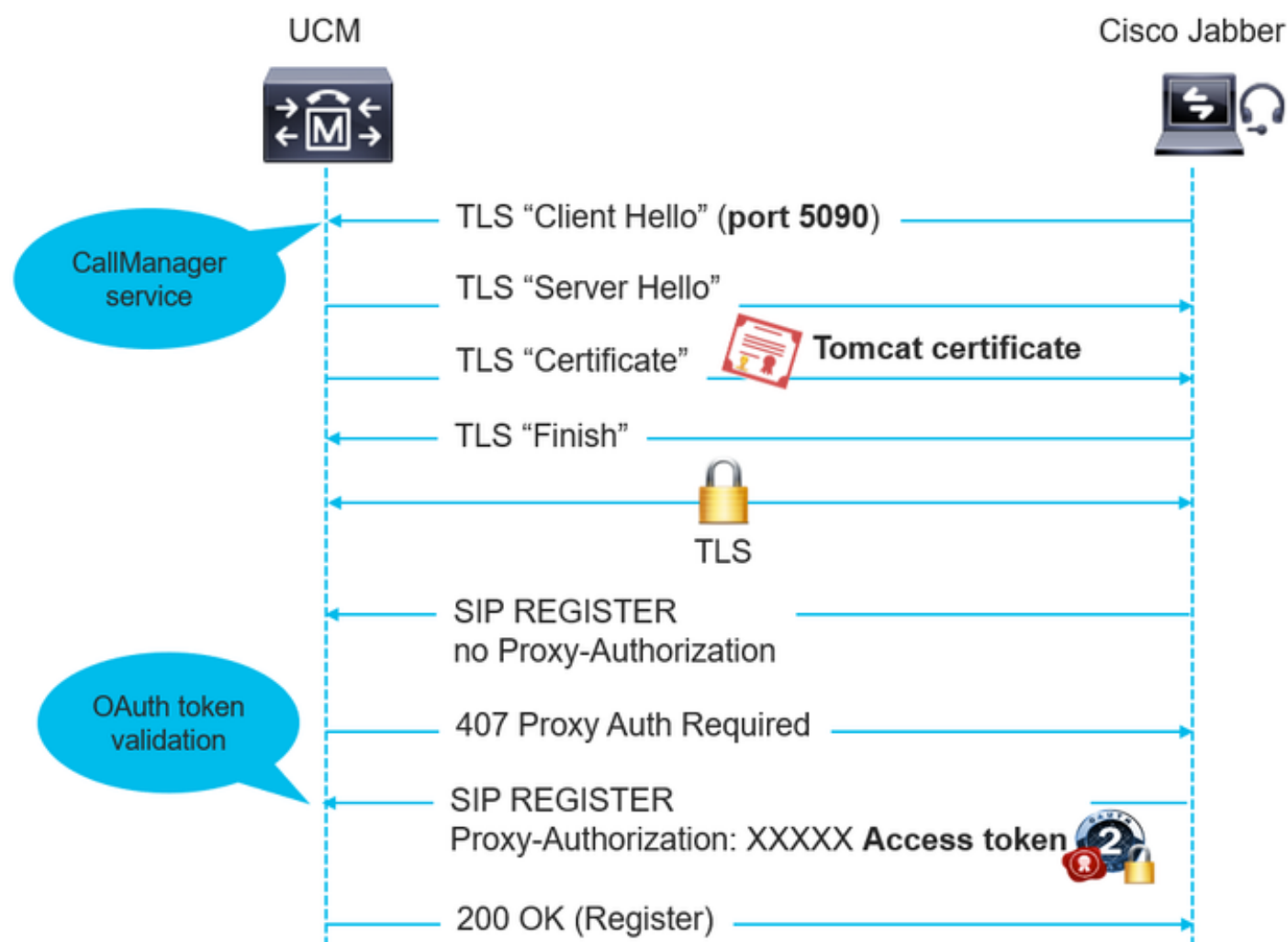
 **Nota:** Cisco UCM utilizza la porta SIP Phone OAuth (5090) per ascoltare la registrazione della linea SIP dai dispositivi Jabber OnPremise su TLS. Tuttavia, UCM utilizza la porta SIP Mobile Remote Access (predefinita 5091) per ascoltare le registrazioni della linea SIP da Jabber su Expressway tramite mLTS. Entrambe queste porte sono configurabili. Vedere la sezione di configurazione.

Il servizio CallManager è in ascolto sia su `sipOAuthPort` che su `sipOAuthPort`. Tuttavia,

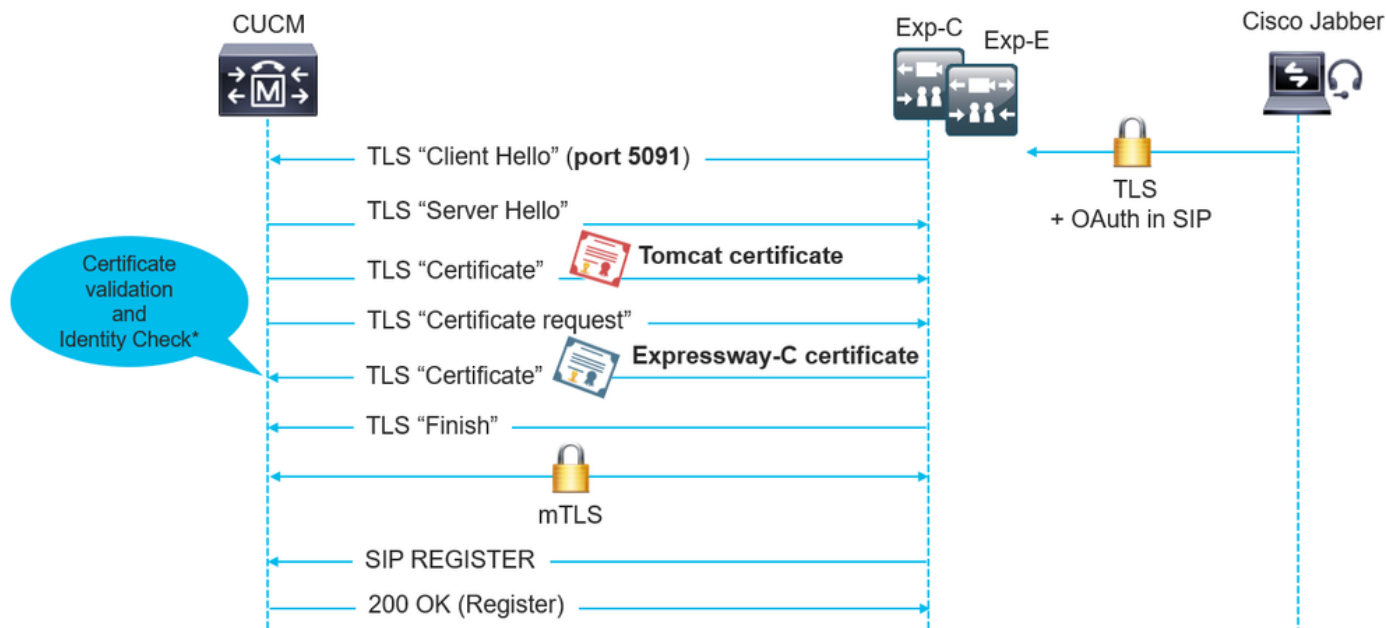
 entrambe le porte utilizzano il certificato Tomcat e Tomcat-trust per le connessioni TLS/mTLS in ingresso. Verificare che l'archivio Tomcat-trust sia in grado di verificare il certificato Expressway-C per la modalità SIP OAuth affinché l'Autorità registrazione integri funzioni correttamente.

In alcuni casi, quando il certificato Tomcat viene rigenerato, è necessario riavviare il processo CallManager anche sui nodi interessati. Questa operazione è necessaria per il caricamento e l'utilizzo di nuovi certificati nelle porte sipOAuth da parte del processo CCM.

Questa immagine mostra la registrazione di Cisco Jabber mentre si trova in locale:



L'immagine mostra la registrazione di Cisco Jabber su MRA:



*I nodi Expressway-C utilizzano l'API AXL per informare l'UCM della CN/SAN nel loro certificato. UCM utilizza queste informazioni per convalidare il certificato Exp-C quando viene stabilita una connessione Mutual TLS.

Configurazione - Jabber locale

- Nota:**
Assicurarsi di aver completato i punti seguenti prima della configurazione della modalità SIP OAuth:
- MRA è configurato e viene stabilita la connessione tra Unified Communications Manager (UCM) ed Expressway (applicabile solo se MRA è in uso).
 - UCM è registrato su un account Smart o Virtual con funzionalità che consentono il controllo delle esportazioni.

1. Configurare i login di aggiornamento.

Configurare gli account di accesso per l'aggiornamento con i token di accesso OAuth e i token di aggiornamento per i client Cisco Jabber. Da Cisco Unified CM Administration, scegliere Sistema > Parametri Enterprise.

SSO and OAuth Configuration	
OAuth Access Token Expiry Timer (minutes) *	60
Jabber OAuth Refresh Token Expiry Timer (days) *	60
Physical Phone OAuth Refresh Token Expiry Timer (days) *	60
Redirect URIs for Third Party SSO Client	
SSO Login Behavior for IOS *	Use embedded browser (WebView)
OAuth with Refresh Login Flow *	Enabled
Use SSO for RTMT *	False

2. Configurare le porte OAuth.

Scegliere Sistema > Cisco Unified CM. Questo passaggio è facoltativo. Nell'immagine vengono visualizzati i valori predefiniti. L'intervallo configurabile accettabile è compreso tra 1024 e 49151. Ripetere la stessa procedura per ogni server.

Cisco Unified Communications Manager TCP Port Settings for this Server	
Ethernet Phone Port*	2000
MGCP Listen Port*	2427
MGCP Keep-alive Port*	2428
SIP Phone Port*	5060
SIP Phone Secure Port*	5061
SIP Phone OAuth Port*	5090
SIP Mobile and Remote Access OAuth Port*	5091

3. Abilitare la modalità OAuth SIP.

Utilizzare l'interfaccia della riga di comando del server di pubblicazione per attivare globalmente la modalità SIP OAuth. Eseguire il comando: utilizza l'abilitazione in modalità sipOAuth.

```
admin:utils sipOAuth-mode enable
SIP OAuth mode enabled.
Please restart the Cisco CallManager service on all nodes in the cluster where it is running.
admin:
```

4. Riavviare il servizio Cisco CallManager.

Da Cisco Unified Serviceability, scegliere Strumenti > Control Center - Feature Services. Selezionare e riavviare il servizio Cisco CallManager su tutti i nodi in cui è attivo.

5. Configurare il supporto OAuth nel profilo di sicurezza.

Da Cisco Unified CM Administration, scegliere Sistema > Profilo sicurezza telefono. Selezionare Abilita autenticazione OAuth per abilitare il supporto OAuth SIP per l'endpoint.

Phone Security Profile Information	
Product Type:	Cisco Unified Client Services Framework
Device Protocol:	SIP
Name*	Cisco Unified Client Services Framework - OAuth auth
Description	Cisco Unified Client Services Framework - OAuth auth
Device Security Mode	Encrypted
Transport Type*	TLS
☐ TFTP Encrypted Config	
☒ Enable OAuth Authentication	

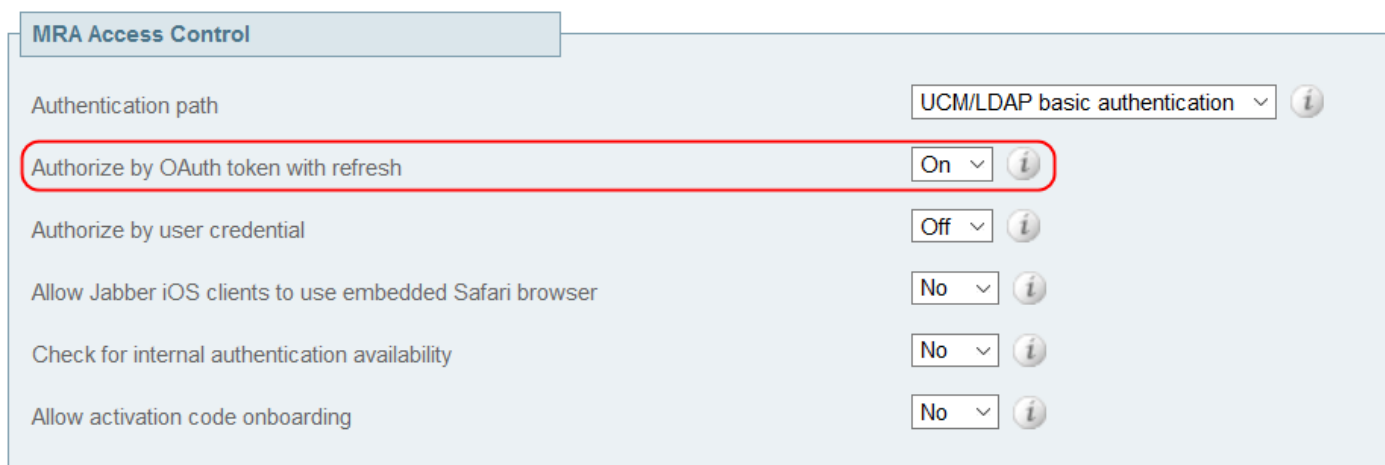
Configurazione - Jabber over MRA

Prerequisiti

Prima di configurare la modalità SIP OAuth per Jabber su MRA, completare i passaggi da 1 a 4 del capitolo Configurazione - Jabber locale di questo articolo.

Passaggio 1. Abilitare Aggiorna login su MRA.

Gli account di accesso per l'aggiornamento devono essere abilitati in Expressway (detti anche token autodescrittivi) prima della configurazione dell'autenticazione OAuth SIP con Cisco Jabber su MRA. In Expressway-C, passare a Configurazione > Comunicazioni unificate > Configurazione e verificare che il parametro Autorizza da token OAuth con aggiornamento sia impostato su Attivato.



MRA Access Control

Authentication path: UCM/LDAP basic authentication ⓘ

Authorize by OAuth token with refresh: On ⓘ

Authorize by user credential: Off ⓘ

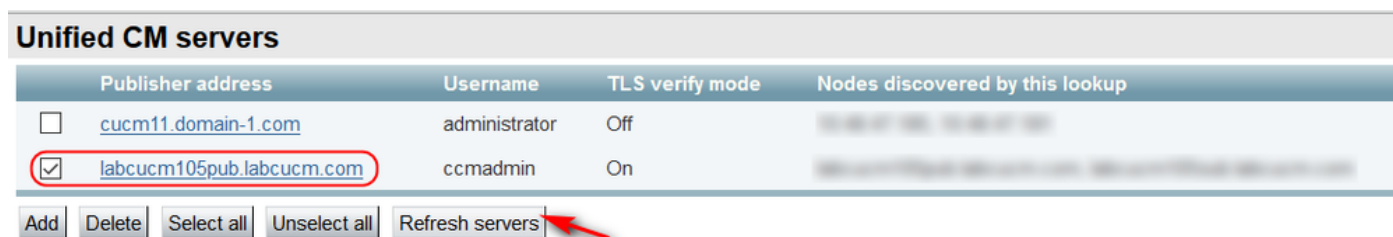
Allow Jabber iOS clients to use embedded Safari browser: No ⓘ

Check for internal authentication availability: No ⓘ

Allow activation code onboarding: No ⓘ

Passaggio 2. Aggiornare i nodi CM unificati in Expressway-C.

Passare a Configurazione > Unified Communications > Unified CM servers (Comunicazioni unificate > Server CM unificato). Individuare o aggiornare i nodi di Unified CM in Expressway-C.



Unified CM servers

	Publisher address	Username	TLS verify mode	Nodes discovered by this lookup
☐	cucm11.domain-1.com	administrator	Off	192.168.1.100, 192.168.1.101
☒	labcucm105pub.labcucm.com	ccmadmin	On	192.168.1.102, 192.168.1.103

Add Delete Select all Unselect all Refresh servers

 Nota: Una nuova zona CEOAuth (TLS) viene creata automaticamente in Expressway-C. Ad esempio, CEOAuth <nome CM unificato>. Viene creata una regola di ricerca per inoltrare le richieste SIP provenienti da Jabber su MRA verso il nodo Unified CM. Questa zona utilizza connessioni TLS indipendentemente dal fatto che la modalità di configurazione di Gestione certificati unificata sia mista o meno. Per stabilire l'attendibilità, Expressway-C invia inoltre i dettagli relativi al nome host e al nome alternativo del soggetto (SAN) al cluster di Gestione

 certificati unificata. Per verificare che sia presente la configurazione corretta, consultare la parte relativa alla verifica di questo articolo.

Passaggio 3. Configurare il supporto OAuth nel profilo di sicurezza.

Da Cisco Unified CM Administration, scegliere Sistema > Profilo sicurezza telefono. Abilitare il supporto OAuth nel profilo assegnato a Cisco Jabber.

Phone Security Profile Information

Product Type:	Cisco Unified Client Services Framework
Device Protocol:	SIP
Name*	Cisco Unified Client Services Framework - OAuth auth
Description	Cisco Unified Client Services Framework - OAuth auth
Device Security Mode	Encrypted
Transport Type*	TLS
☐ TFTP Encrypted Config	
☒ Enable OAuth Authentication	

Verifica

1. Verificare se la modalità OAuth SIP è abilitata a livello globale.

Verificare la modalità OAuth da Cisco Unified CM Administration, scegliere Sistema > Parametri Enterprise.

Security Parameters

Cluster Security Mode *	1
Cluster SIPOAuth Mode *	Enabled
LBM Security Mode *	Insecure

In alternativa, utilizzare Admin CLI - Eseguire il comando: run sql select paramvalue FROM processconfig WHERE paramname = 'ClusterSIPOAuthMode'

```
admin:run sql select paramvalue FROM processconfig WHERE paramname = 'ClusterSIPOAuthMode'
paramvalue
=====
1
admin:
```

Valori possibili: 0 - per Disabilitato (Predefinito), 1 - per Abilitato.

2. Verificare che le voci SAN Expressway-C siano state inserite correttamente in CUCM.

Expressway-C invia i dettagli CN/SAN del proprio certificato a UCM tramite AXL. Tali dettagli vengono salvati nella tabella di configurazione expressway. Questo processo viene richiamato ogni volta che si individuano o si aggiornano i nodi CM unificati in Expressway-C. Queste voci vengono utilizzate per stabilire la relazione di trust tra UCM ed Expressway-C. Il campo CN/SAN del certificato Expressway-C viene confrontato con tali voci durante la connessione MTLS alla porta SIP MRA OAuth (5091 per impostazione predefinita). Se la verifica ha esito negativo, la connessione MTLS non riesce.

Verificare le voci da Cisco Unified CM Administration, scegliere Dispositivo > Expressway-C (disponibile da UCM 12.5.1Su1 in avanti)

Cisco Expressway-C Configuration

Host Name/IP Address*	exp-c
Description	this is added through axl
X509 Subject Name / Subject Alternate Name	domain-2.com, domain-1.com, exp-c.domain-1.com

In alternativa, utilizzare Admin CLI - Eseguire il comando: `run sql select * from expressway configuration`

```
admin:run sql select * from expresswayconfiguration
pkid                               hostnameorip  description                               x509subjectnameoraltname
=====
d5fd15d5-b049-c5b5-0197-bd11a5641640 exp-c        this is added through axl domain-2.com,secure-phone-profile,domain-1.com,exp-c.domain-1.com
admin:
```

3. Verificare le zone CEOAuth in Expressway-C.

Passare a Expressway-C > Configurazione > Zone > Zone. Verificare che tutte le zone CEOAuth appena create siano in stato attivo.

Name ▾	Type	Calls	Bandwidth used	H323 status	SIP status
DefaultZone	Default zone	0	0 kbps	Off	On
CEOAuth-	Neighbor	0	0 kbps	Off	Active
CEOAuth-	Neighbor	0	0 kbps	Off	Active

4. Verificare che il processo CallManager sia in ascolto sulle porte SIP OAuth.

Eseguire il comando dalla CLI di amministrazione: `show open ports regexp 5090` (porta SIP OAuth predefinita)

```
admin:show open ports regexp 5090

Executing.. please wait.
ccm      30622    ccmbase  364u  IPv4  207160      0t0  TCP  10.48.10.10:5090 (LISTEN)
```

Eseguire il comando dalla CLI di amministrazione: `show open ports regexp 5091` (porta OAuth SIP MRA predefinita)

```
admin:show open ports regexp 5091
```

```
Executing.. please wait.
```

```
ccm      30622      ccmbase  351u  IPv4  207155      0t0  TCP  10.48. :5091 (LISTEN)
```

Risoluzione dei problemi

Esempio di registro Jabber (locale)

Esempio di log per la registrazione SIP OAuth locale sulla porta 5090 dalla prospettiva di log di Jabber.

```
## CSF configuration retrieved 2020-03-30 13:03:18,278 DEBUG [0x000012d8]
```

```
[src\callcontrol\ServicesManager.cpp(993)] [csf.ecc] [csf::ecc::ServicesManager::fetchDeviceConfig] -  
fetchDeviceConfig() retrieved config for CSFrado 2020-03-30 13:03:18,278 DEBUG [0x000012d8]
```

```
[rc\callcontrol\ServicesManager.cpp(1003)] [csf.ecc] [csf::ecc::ServicesManager::fetchDeviceConfig] -  
Device Config:
```

10.10.10.1

ccm12pub

2000

5060

5061

5090

5091

...

1

```
## Setting SIP oauth mode to 1 2020-03-30 13:03:18,747 DEBUG [0x00002968]
```

[ig\CertificateVerificationHelper.cpp(35)] [csf.ecc]
[csf::ecc::CertificateVerificationHelper::setSipOAuthMode] - sip OAuth Mode=1 ## Setting OAuth ports
(5090 and 5091) for each UCM server 13:03:19,013 INFO [0x00002484]
[core\ccapp\config\config_parser.c(1491)] [csf.sip-call-control] [config_process_ccm_properties] -
ccm0=10.10.10.1 ccm1=10.10.10.2 ccm2= sip_oauth_port_0=5090 sip_oauth_port_1=5090
sip_oauth_port_2=5090 length=0 13:03:19,013 INFO [0x00002484]
[core\ccapp\config\config_parser.c(1494)] [csf.sip-call-control] [config_process_ccm_properties] -
sip_mar_oauth_port_0=5091 sip_mar_oauth_port_1=5091 sip_mar_oauth_port_2=5091 ## Open TLS
connection to 5090 2020-03-30 13:03:18,528 DEBUG [0x00000e2c]
[sipstack\sip_transport_connection.c(431)] [csf.sip-call-control] [sip_create_transport_connection] -
[SIP][CONN][0] create TLS connection 10.10.10.10:5061-----10.10.10.1:5090. ## Sending register message
2020-03-30 13:03:19,200 DEBUG [0x00000e2c] [\sipcc\core\sipstack\ccsip_debug.c(1041)] [csf.sip-call-
control] [platform_print_sip_msg] - sipio-sent---> REGISTER sip:10.10.10.1 SIP/2.0 Via: SIP/2.0/TLS
10.10.10.10:62162;branch=z9hG4bK00001188 From:

;tag=882323451234089000003bdd-00005eff To:

Call-ID: 88232345-12340017-00001c0b-00000cfa@10.10.10.10 Max-Forwards: 70 Date: Mon, 30
Mar 2020 11:03:19 GMT CSeq: 2270 REGISTER User-Agent: Cisco-CSF Contact:

;+sip.instance="

";+u.sip!devicename.ccm.cisco.com="CSFrado";+u.sip!model.ccm.cisco.com="503";video
Supported: replaces,join,sdp-anat,norefersub,resource-priority,extended-refer,X-cisco-callinfo,X-cisco-
serviceuri,X-cisco-escapecodes,X-cisco-service-control,X-cisco-srtp-fallback,X-cisco-monrec,X-cisco-
config,X-cisco-sis-7.0.0,X-cisco-xsi-8.5.1,X-cisco-graceful-reg,X-cisco-duplicate-reg ## 407 Proxy
Authentication Required 2020-03-30 13:03:19,310 DEBUG [0x00000e2c]
[\sipcc\core\sipstack\ccsip_debug.c(1041)] [csf.sip-call-control] [platform_print_sip_msg] - sipio-recv<---
SIP/2.0 407 Proxy Authentication Required Via: SIP/2.0/TLS
10.10.10.10:62162;branch=z9hG4bK00001188 From:

;tag=882323451234089000003bdd-00005eff To:

;tag=441122775 Date: Mon, 30 Mar 2020 11:03:31 GMT Call-ID: 88232345-12340017-
00001c0b-00000cfa@10.10.10.10 Server: Cisco-CUCM12.5 CSeq: 2270 REGISTER Proxy-Authenticate:
Bearer realm="ccmsipline" Content-Length: 0 ## Register with OAuth token included in the Proxy-
Authorization header 2020-03-30 13:03:19,310 DEBUG [0x00000e2c]
[\sipcc\core\sipstack\ccsip_debug.c(1041)] [csf.sip-call-control] [platform_print_sip_msg] - sipio-sent--->
REGISTER sip:10.10.10.1 SIP/2.0 Via: SIP/2.0/TLS 10.10.10.10:62162;branch=z9hG4bK00004a82 From:

;tag=882323451234089000003bdd-00005eff To:

Call-ID: 88232345-12340017-00001c0b-00000cfa@10.10.10.10 Max-Forwards: 70 Date: Mon,
30 Mar 2020 11:03:19 GMT CSeq: 2271 REGISTER User-Agent: Cisco-CSF Contact:

;+sip.instance="

";+u.sip!devicename.ccm.cisco.com="CSFrado";+u.sip!model.ccm.cisco.com="503";video
Proxy-Authorization: Bearer token="

" Supported: replaces,join,sdp-anat,norefersub,resource-priority,extended-refer,X-cisco-callinfo,X-cisco-serviceuri,X-cisco-escapecodes,X-cisco-service-control,X-cisco-srtp-fallback,X-cisco-monrec,X-cisco-config,X-cisco-sis-7.0.0,X-cisco-xsi-8.5.1,X-cisco-graceful-reg,X-cisco-duplicate-reg
Reason: SIP;cause=200;text="cisco-alarm:111 Name=CSFrado ActiveLoad=Jabber_for_Windows-12.8.0.51973 InactiveLoad=Jabber_for_Windows-12.8.0.51973 Last=Application-Requested-Destroy"
Expires: 3600 Content-Type: multipart/mixed; boundary=uniqueBoundary Mime-Version: 1.0 Content-Length: 1271 # 200 OK for Register 2020-03-30 13:03:19,325 DEBUG [0x00000e2c]
[sipcc\core\sipstack\ccsip_debug.c(1041)] [csf.sip-call-control] [platform_print_sip_msg] - sipio-recv<---
SIP/2.0 200 OK Via: SIP/2.0/TLS 10.10.10.10:62162;branch=z9hG4bK00004a82 From:

;tag=882323451234089000003bdd-00005eff To:

;tag=1915868308 Date: Mon, 30 Mar 2020 11:03:31 GMT Call-ID: 88232345-12340017-00001c0b-00000cfa@10.10.10.10 Server: Cisco-CUCM12.5 CSeq: 2271 REGISTER Expires: 120 Contact:

;+sip.instance="

";+u.sip!devicename.ccm.cisco.com="CSFrado";+u.sip!model.ccm.cisco.com="503";video;x-cisco-newreg
Supported: X-cisco-srtp-fallback,X-cisco-sis-9.1.0 Content-Type: application/x-c

Scenario 1 - Mancata corrispondenza della porta di registrazione SIP OAuth

Il dispositivo Jabber in locale in modalità SIP OAuth non riesce a eseguire la registrazione con UCM. UCM invia 403 per il messaggio Register:

SIP/2.0 403 Forbidden Via: SIP/2.0/TLS 10.5.10.121:50347;branch=z9hG4bK00005163 From:

;tag=005056867e66010a00006698-00002a32 To:

;tag=1946377502 Date: Fri, 03 Aug 2018 05:00:18 GMT Call-ID: 00505686-7e660005-0000216b-0000366f@10.5.10.121 Server: Cisco-CUCM12.5 CSeq: 363 REGISTER Retry-After: 35 Warning: 399 UCM2-PUB "SIP OAuth Registration port Mismatch" Content-Length: 0

Soluzione possibile: Assicurarsi che siano soddisfatte le seguenti condizioni:

- La modalità OAuth è abilitata a livello globale
- Il profilo di sicurezza del dispositivo associato al dispositivo ha il supporto OAuth abilitato
- Messaggio ricevuto sulla porta 5090 su TLS anziché su mTLS

Scenario 2 - CA sconosciuta da Expressway

Expressway-C non è in grado di stabilire l'handshake mTLS con UCM su sipMRAOAuthport (predefinito: 5091). Expressway-C non considera attendibile il certificato condiviso da UCM e risponde con il messaggio Autorità di certificazione sconosciuta durante l'installazione di MTL.

Soluzione possibile: Il servizio CallManager invia il certificato Tomcat durante l'handshake mTLS. Verificare che Expressway-C sia attendibile per il firmatario del certificato Tomcat di UCM.

Scenario 3 - CA sconosciuta da UCM

Expressway-C non è in grado di stabilire l'handshake mTLS con UCM su sipMRAOAuthport (predefinito: 5091). UCM non considera attendibile il certificato condiviso da Expressway e risponde con il messaggio Autorità di certificazione sconosciuta durante l'installazione di mTLS.

Acquisizione pacchetti da questa comunicazione (UCM 10.x.x.198, Expressway-C 10.x.x.182):

Time	Source	Destination	Protocol	Source port	Destination	Length	Info
11:16:29.659235	10.48.47.182	10.48.53.198	TCP	25161 5091	74 25161 → 5091		[SYN] Seq=0 Win=64240 Len=0 MSS=1
11:16:29.659609	10.48.53.198	10.48.47.182	TCP	5091 25161	74 5091 → 25161		[SYN, ACK] Seq=0 Ack=1 Win=28960
11:16:29.659627	10.48.47.182	10.48.53.198	TCP	25161 5091	66 25161 → 5091		[ACK] Seq=1 Ack=1 Win=64256 Len=0
11:16:29.714501	10.48.47.182	10.48.53.198	TLSv1.2	25161 5091	260		Client Hello
11:16:29.715316	10.48.53.198	10.48.47.182	TCP	5091 25161	66 5091 → 25161		[ACK] Seq=1 Ack=195 Win=30080 Len=
11:16:29.737063	10.48.53.198	10.48.47.182	TLSv1.2	5091 25161	1514		Server Hello
11:16:29.737091	10.48.47.182	10.48.53.198	TCP	25161 5091	66 25161 → 5091		[ACK] Seq=195 Ack=1449 Win=64128
11:16:29.737137	10.48.53.198	10.48.47.182	TLSv1.2	5091 25161	1081		Certificate, Server Key Exchange, Certificate
11:16:29.737149	10.48.47.182	10.48.53.198	TCP	25161 5091	66 25161 → 5091		[ACK] Seq=195 Ack=2464 Win=63488
11:16:29.753375	10.48.47.182	10.48.53.198	TLSv1.2	25161 5091	2878		Certificate, Client Key Exchange, Certificate
11:16:29.754116	10.48.53.198	10.48.47.182	TCP	5091 25161	66 5091 → 25161		[ACK] Seq=2464 Ack=3007 Win=35712
11:16:29.758710	10.48.53.198	10.48.47.182	TLSv1.2	5091 25161	73		Alert (Level: Fatal, Description: Unknown CA)
11:16:29.758743	10.48.47.182	10.48.53.198	TCP	25161 5091	66 25161 → 5091		[ACK] Seq=3007 Ack=2471 Win=64128
11:16:29.758780	10.48.53.198	10.48.47.182	TCP	5091 25161	66 5091 → 25161		[RST, ACK] Seq=2471 Ack=3007 Win=

Soluzione possibile: UCM utilizza l'archivio Tomcat-trust per verificare i certificati in ingresso durante l'handshake mTLS sulle porte SIP OAuth. Verificare che il certificato del firmatario per

Expressway-C sia caricato correttamente nell'UCM.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).